WHAT IS CLAIMED IS:

1. A modular multiplier, capable of processing a first operand and a second operand in relation to a modulus for performing a modular multiplication operation, the performed operation including an instruction, which has an internal multiplication and addition operation with inner recursion and an external multiplication and addition operation, the modular multiplier comprising:

a first buffer device for storing the first operand, wherein the first operand is divided into a first plurality of sub-operands with fixed length;

a second buffer device for storing the second operand, wherein the second operand is divided into a second plurality of sub-operands with fixed length;

a third buffer device for storing the parameter of the modular multiplication operation;

a multiplexer device coupled to the first, the second, and the third buffer devices, for choosing a first multiplication operand and a second multiplication operand from the first sub-operand, the second sub-operand, and the parameter according to the required internal and external multiplication/addition operations;

a multiplication device coupled to the multiplexer device, for multiplying the first multiplication operand by the second multiplication operand to obtain a product; and

an addition device coupled to the multiplication device, for outputting an intermediate result according to the product during the internal multiplication and addition operation and outputting the result of the modular multiplication operation according to the product and the

intermediate result during the external multiplication and addition operation.

2. The modular multiplier of Claim 1, wherein the addition device further comprises:

a first delay component coupled to the multiplication device, for receiving half of the product at the lower-bit portion;

a second delay component coupled to the multiplication device, for receiving half of the product at the higher-bit portion, wherein the second delay component has a multiplication clock more than the first delay component; and

an adder coupled to the first delay component and the second delay component, for receiving intermediate values from the first and second delay components to perform the addition operation.

3. The modular multiplier of Claim 1, further comprising an encryption processor for encrypting a plaintext using an encryption key according to a modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

4. The modular multiplier of Claim 3, further comprising a decryption processor for decrypting a ciphertext using a decryption key according to the modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

5. The modular multiplier of Claim 1-, further comprising a smart card having an encryption/decryption processor for encrypting/decrypting internal data, wherein the encryption/decryption processor performs the encryption/decryption using an encryption/decryption key according to a modular exponentiation operation, and the modular exponentiation operation is performed by the multiplier.

6. A modular multiplier, capable of processing a first operand and a second operand in relation to a modulus for performing a modular multiplication operation, the performed operation including an external loop and an internal loop, the internal loop having an instruction, which has an internal multiplication and addition operation with inner recursion and an external multiplication and addition operation, the modular multiplier comprising:

a first buffer device for storing the first operand, wherein the first operand is divided into a first plurality of sub-operands with fixed length, each sub-operand respective to the external loop;

a second buffer device for storing the second operand, wherein the second operand is divided into a second plurality of sub-operands with fixed length, each sub-operand respective to the internal loop;

a third buffer device for storing a first and a second parameters of the modular multiplication operation;

a multiplexer device coupled to the first, the second, and the third buffer devices, for choosing a first multiplication operand and a second multiplication operand, which are selected from one of the two groups, the first sub-operand and parameter and the second sub-operand and

parameter according to the required internal and external multiplication/addition operations;

a multiplication device coupled to the multiplexer device, for multiplying the first multiplication operand by the second multiplication operand to obtain a product;

an addition device coupled to the multiplication device, for outputting an intermediate result according to the product during the internal multiplication and addition operation and outputting the result of the modular multiplication operation according to the product and the intermediate result during the external multiplication and addition operation; and

a controller for outputting a control signal to control the multiplexer.

7. The modular multiplier of Claim 6, wherein the addition device further comprises:

a first delay component coupled to the multiplication device, for receiving half of the product at the lower-bit portion;

a second delay component coupled to the multiplication device, for receiving half of the product at the higher-bit portion, wherein the second delay component has a multiplication clock more than the first delay component; and

an adder coupled to the first delay component and the second delay component, for receiving intermediate values from the first and second delay components to perform the addition operation.

8. The modular multiplier of Claim 6, further comprising an encryption processor for encrypting a plaintext using an encryption key according to a modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

9. The modular multiplier of Claim 8, further comprising a decryption processor for decrypting a ciphertext using a decryption key according to the modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

10. The modular multiplier of Claim 6, further comprising a smart card having an encryption/decryption processor for encrypting/decrypting internal data, wherein the encryption/decryption processor performs the encryption/decryption using an encryption/decryption key according to a modular exponentiation operation, and the modular exponentiation operation is performed by the multiplier.